

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



NICS Portal Screenshots
Peggy Maxson



Human Capital Managers: Effective Strategies to Build Your Cybersecurity Workforce

What's your HC Strategy? Hiring, retaining and sustaining an effective, proactive Cybersecurity function presents challenges to HCMs, learn what you need to do to develop a successfully strategy...



Information for

The Nation
General Public
Students
Educators
Parents

Industry
Cybersecurity Professionals
Human Capital Managers
Cyber Managers

Government
Cybersecurity Professionals
Human Capital Managers
Cyber Managers
Policy Makers

Veterans



STOP | THINK | CONNECT™

Cybersecurity is a shared responsibility. For additional tips and resources for all age groups, visit the Department of Homeland Security's Stop.Think.Connect™ Campaign.



STAY SAFE

Cybersecurity is for everyone. Awareness is the first step, explore tips & strategies to keep yourself and your family safe.



FIND TRAINING

Our automated tool can match you with the professional training you need to keep up with changing threats.



EXPLORE CAREERS

Explore the 31 Cybersecurity Specialty Areas defined within the National Cybersecurity Workforce Framework.



WORKFORCE DEVELOPMENT

Learn about skills gap analysis, training strategies, and other activities to keep your Cyber workforce on top.



DISCOVER EDUCATIONAL OPPORTUNITIES

A Cybersecurity career can begin at different stages. From grade school to graduate school, explore educational opportunities on the CYBER HIGHWAY.

UPCOMING EVENTS

JUN 11 CISSE
June 11 - 13
Lake Buena Vista, FL

JUN 18 Cyber Discovery Camp 1.0
Jun 18 - 23
Baltimore, MD

JUL 9 Cyber Discovery Camp 2.0
Jul 9 - 14
Ruston, LA

AUG 19 GFIRST
Aug 19-24
Atlanta, GA

AUG 28 Information Assurance
Exposition
August 28-30
Nashville, TN

SEP 10 ISC2 Security Congress
Sept 10 - 13
Philadelphia, PA

OCT 1 National Cyber Security
Awareness Month
Oct 1 - Oct 30

OCT 30 NICE Workshop
Oct 30 - Nov 1
Gaithersburg, MD

NOV 11 CAE Principles Meeting
Nov 11 - 13
Atlanta, GA

[VIEW CALENDAR](#)
[SUBMIT AN EVENT](#)



Education Resources

Information for Students and Educators, from P-12, Undergrad to Doctoral Candidate:

Discover Innovative Programs
Explore Degree Programs
Find Cyber Competitions
Find Scholarships



Training Resources

Tools to connect Cybersecurity Professionals and Training Opportunities:

Find Training Opportunities
Explore the Workforce Framework
Explore Professional Certifications
Map & Submit Training Opportunities



Talent Management

Career development and HR Resources for Cyber Professionals and HR Professionals:

Understanding Professionalization
Explore Career Roadmaps



Research

Whitepapers, studies and other research promoting Cybersecurity education and the Profession.

Search NICE Research
Submit Research

I Want To...

Become a Cyber Professional
Advance my Cyber Career
Explore the NICE Framework
Search for Training Courses
Get my child involved
Become a NICE Partner
Become a Training Catalog Vendor

NICE Partners



NIST



NICS

National Institute for Cybersecurity Studies

About NICS | A-Z Site Map



HOME

AWARENESS

EDUCATION

TRAINING

CAREERS

NEWS & EVENTS

RESEARCH

COMMUNITY

AWARENESS

[Awareness Home](#)

[How-to Guide](#)

[Cyber Glossary](#)

[NICE Initiatives](#)



STOP | THINK | CONNECT

Cybersecurity is a shared responsibility. For additional tips and resources for all age groups, visit the Department of Homeland Security's Stop Think Connect™ Campaign.



BEST PRACTICES

View our Cyber How-To Guide to learn safe online strategies and find additional Awareness resources.



CYBER TERMS

View our Interactive Cyber Glossary to learn Cybersecurity Terminology and learn about DHS effort to standardize terms.



PROMOTING SAFETY

Learn about NICE initiatives to promote Awareness at work and at home.



CELEBRATE AWARENESS

October is National Cyber Security Awareness Month. See what's going on.

Why Cybersecurity Awareness?

More than ever, people rely on the internet for everything from bank communications, to making transportation reservations, to entertainment. With each click of the mouse, citizens risk their online security if they have not taken the proper precautions to protect themselves and their Personally Identifiable Information (PII). Cybersecurity involves protecting that information by preventing, detecting, and responding to attacks.

Cybersecurity is a growing issue. Our vulnerabilities threaten the safety and livelihood of our citizens' online safety and as such, it is paramount that the government work to increase the public's awareness of cybersecurity and make them active and involved cybercitizens. [Learn about ongoing initiatives](#) to promote Awareness for all Americans.

What Can I do to Protect Myself?

While there are no sure ways to protect yourself from a cyber attack, there are some simple steps you can take to help keep your PII private.

- Set secure passwords and don't share them with anyone. Avoid using common words, phrases, or personal information and update regularly.
- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Verify the authenticity of requests from companies or individuals by contacting them directly. If you are being asked to provide personal information via email, you can independently contact the company directly to verify this request.
- Pay close attention to website URLs. Pay attention to the URLs of websites you visit. Malicious websites sometimes use a variation in common spelling or a different domain (for example, .com instead of .net) to deceive unsuspecting computer users.
- For additional tips visit [STOP|THINK|CONNECT](#) and view our [How-to Guide](#).



The government has a number of resources available to the public to learn more about protecting yourself. Get more cybersecurity tips from DHS specific to email, phone, and social media among others, at <http://www.dhs.gov/files/electronic/cybersecurity.tips.shtml>. Get additional tips through US-CERT at <http://www.us-cert.gov/ocs/links>.

Increase Your Awareness

[STOP|THINK|CONNECT](#)

[Stay Safe Online](#)

[National Cyber Security Awareness Month](#)

[OnGuardOnline.gov](#)



I Want To...

[Become a Cyber Professional](#)
[Advance my Cyber Career](#)
[Explore the NICE Framework](#)
[Search for Training Courses](#)
[Get my child involved](#)
[Become a NICE Partner](#)
[Become a Training Catalog Vendor](#)

Promoting Cybersecurity Safety at Work and at Play

AWARENESS TIPS

Provided by US-CERT

ST00-001: Holiday Traveling with Personal Internet-Enabled Devices

Tuesday, March 20, 2012, 10:10:20 AM

The internet is at our fingertips with the widespread use of internet-enabled devices such as smart phones and tablets. When traveling and shopping systems, and especially during the holidays, consider the wireless network you are using when you complete transactions on your device.

ST00-001: Understanding Hidden Threats: Rootkits and Botnets

Tuesday, March 20, 2012, 10:10:20 AM

Attackers are continually finding new ways to access computer systems. The use of hidden methods such as rootkits and botnets has increased, and you may be a victim without even realizing it.

ST00-002: Understanding ISPs

Tuesday, March 20, 2012, 10:10:20 AM

ISPs offer services like email and internet access. In addition to availability, you may want to consider other factors as that you find an ISP that supports all of your needs.

ST00-003: Dealing with Cyberattacks

Tuesday, March 20, 2012, 10:10:20 AM

Bad guys are taking advantage of technology to intimidate and harass their victims. Dealing with cyberattacks can be difficult, but there are steps you can take.

ST00-002: Keeping Children Safe Online

Tuesday, March 20, 2012, 10:10:20 AM

Children present unique security risks when they use a computer—not only do you have to keep them safe, you have to protect the data on your computer. By taking some simple steps, you can dramatically reduce the threat.

ST00-001: Using Caution with USB Drives

Tuesday, March 20, 2012, 10:10:20 AM

USB drives are popular for storing and transporting data, but some of the data stored that make them so convenient also introduce security risks.

[MORE](#)

NICE Partners





EDUCATION

Furthering Learning in Cybersecurity & STEM

Education Home

For Students

- Degree Programs
- Scholarship Opportunities
- Hands On Learning Activities
- Cyber Competitions
- Cyber Camps

For Educators

NICE Initiatives

- STEM Improvement Efforts
- Common Evidence Standards
- Promoting Education
- Curriculum Resources
- Virtual Labs

Programs

- Software Assurance
- Centers of Academic Excellence (CAE)
- Regional Cyber Centers
- I-Corps
- Scholarship for Service (SFS)
- Integrated Cybersecurity Education Communities (ICEC)
- Cyber Competitions
- Investigation Project (CCIP)



CLASSROOM LEARNING

Get started with Cybersecurity. Learn about the exciting programs available at every level, from grade school to graduate school.



TEACHING

Get new ideas for bringing technology into the classroom, find curriculum resources and strategies for making STEM accessible.



HANDS ON EXPERIENCES

Find camps, competitions and other after-school activities that extend learning beyond the classroom.



DRIVING INNOVATION

Learn about NICE Initiatives and programs underway to connect Educators, Students and Technology.

Why promote Cybersecurity & STEM Education?

Personal digital security is critical to the Nation's economy and the security of our critical infrastructure. Improving the cybersecurity posture of the nation requires requires change and education at the individual level, from grade school to graduate school and beyond. We must build a digitally literate workforce that uses technology in a secure manner. To do so, we must teach science, technology, engineering and math (STEM) and other critical subjects to all students, and educate all students on the secure use of today's evolving technologies.

It is important to have the educational resources in place to make digital literacy and personal security reality. The Department of Education and the National Science Foundation (NSF) lead the [Formal Cybersecurity Education efforts](#) for NICE. Their mission is to bolster formal cybersecurity education programs encompassing kindergarten through 12th grade, higher education and vocational programs, with a focus on the STEM disciplines to provide a pipeline of skilled workers for the private sector and government.

EDUCATION NEWS

Provided by the [National Science Foundation](#)

NSF Releases Report Detailing Substantial Growth in Graduate Enrollment in Science and Engineering in the Past Decade
Released June 1, 2012
Press Release



Colorado State University Named Under Preparation Network Honored with National Land Grant Organization Award
Released May 25, 2012
News From the Field



NSF Report Details Federal Science and Engineering Support to Colleges, Universities and Nonprofit Institutions
Released May 22, 2012
Press Release



National Science Foundation Hosts Inaugural Global Summit on NICE Review
Released May 16, 2012
Press Release



Duke's "Launch" at National Science Foundation on Thursday, May 24th
Released May 11, 2012
Media Release



NSF Honors Two Early Career Researchers With Alan T. Waterman Award
Released May 10, 2012
Press Release



Engineering Students Using Such Design Tools as SMART Boards Are More Successful
Released May 10, 2012
News From the Field

[MORE](#)



Education Opportunities

- Centers of Academic Excellence
- Advanced Technological Education (ATE) Centers
- Regional Cyber Centers
- Integrated Cybersecurity Education Communities (ICEC)
- National Cybersecurity Education Council (NCEC)

NICS Education Partners

- Stay Safe Online
- Cyber Security Education Consortium (CSEC)
- Center for Systems Security and Information Assurance (CSSIA)
- DHS NCSS Software Assurance

I Want To...

- Become a Cyber Professional
- Advance my Cyber Career
- Explore the NICE Framework
- Search for Training Courses
- Get my child involved
- Become a NICE Partner
- Become a Training Catalog Vendor

NICE Partners





Education Home

For Students

- Degree Programs
- Scholarship Opportunities
- Hands On Learning Activities
- Cyber Competitions
- Cyber Camps

For Educators

NICE Initiatives

- STEM Improvement Efforts
- Common Evidence Standards
- Promoting Education
- Curriculum Resources
- Virtual Labs

Programs

- Software Assurance
- Centers of Academic Excellence (CAE)
- Regional Cyber Centers
- I-Corps
- Scholarship for Service (SF S)
- Integrated Cybersecurity Education Communities (ICEC)
- Cyber Competitions
- Investigation Project (CCIP)

Education > NICE Initiative > ICEC

INTEGRATED CYBERSECURITY EDUCATION COMMUNITIES (ICEC)

ICEC Background

The Nation's cyber infrastructure depends on well-trained Information Technology (IT) professionals to support the systems and networks necessary for essential computer operations. The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Cyber Education Office (CEO) launched ICEC to enhance formal cybersecurity education with the ultimate goal to promote growth of the cybersecurity workforce. DHS believes that by encouraging interest in the cybersecurity field, increasing awareness of cybersecurity careers and academic pathways, and giving teachers tools to teach their students about the availability of related career opportunities, the number of young people who will benefit - and who will consider entering the field of cybersecurity - will be multiplied.

PROJECT OVERVIEW

ICEC is designed to encourage interest in the cybersecurity field, increase awareness of cybersecurity careers and academic pathways, and give teachers tools to teach their students about the availability of related career opportunities.

The ICEC project targets the U.S. high school student population through professional development of high school teachers and cybersecurity education summer camps. ICEC focuses its efforts on training teachers to use project-based learning when integrating cybersecurity content into math, science, and humanities studies. ICEC develops cybersecurity education communities of students and educators, where high school students can hone their cybersecurity skills and teachers simultaneously learn innovative cybersecurity integration techniques.

ICEC sponsors cybersecurity education summer camps, which encourage interest in the cybersecurity field through project-based cyber learning experiences for high school students as well as access to cybersecurity-integrated learning tools for their teachers. Through these camps, ICEC hopes to create an environment in multiple U.S. communities in which science, technology, engineering and mathematics (STEM)-capable students can learn more about cybersecurity, hone their knowledge and skills, and become introduced to the world of cybersecurity.

Through professional development, their experience at the Camp, and online access to cybersecurity curricula, ICEC project high school teachers are equipped to bring cybersecurity principals to their classrooms.

ICEC GOALS & OBJECTIVES

ICEC aims to reach and affect 1.7 million U.S. high school students over 10 years through the cybersecurity education summer camps and teachers integrating cybersecurity content in the classroom. More specifically, ICEC intends to:

1. Provide tools to help high school teachers and their communities contribute to an expanding the pipeline of cybersecurity professionals entering the Nation's workforce.
2. Educate teachers and students in cybersecurity through the summer camps, where STEM-capable students can learn and become introduced to cybersecurity.
3. Provide a portable model to aid in replication of this model to additional U.S. communities.
4. Develop an effectiveness measurement plan to gauge the lasting effects of the model both in the classroom and in the cybersecurity field.



I Want To...

- Become a Cyber Professional
- Advance my Cyber Career
- Explore the NICE Framework
- Search for Training Courses
- Get my child involved
- Become a NICE Partner
- Become a Training Catalog Vendor

Education Opportunities

- Centers of Academic Excellence
- Advanced Technological Education (ATE) Centers
- Regional Cyber Centers
- Integrated Cybersecurity Education Communities (ICEC)

NICS Education Partners

- Stay Safe Online
- Cyber Security Education Consortium (CSEC)
- Center for Systems Security and Information Assurance (CSSIA)
- DHS NCSD Software Assurance

NICE Partners



NIST



Education Home

For Students

[Degree Programs](#)
[Scholarship Opportunities](#)
[Hands-On Learning Activities](#)
[Cyber Competitions](#)
[Cyber Camps](#)

For Educators

NICE Initiatives

[STEM Improvement Efforts](#)
[Common Evidence Standards](#)
[Promoting Education](#)
[Curriculum Resources](#)
[Virtual Labs](#)

Programs

[Software Assurance](#)
[Centers of Academic Excellence \(CAE\)](#)
[Regional Cyber Centers](#)
[I-Camps](#)
[Scholarship for Service \(SFS\)](#)
[Integrated Cybersecurity Education Communities \(ICEC\)](#)
[Cyber Competitions Investigation Project \(CCIP\)](#)

Education > NICE Initiative > CCIP

CYBERSECURITY COMPETITIONS INVESTIGATION PROJECT (CCIP)

CCIP—BUILDING TOMORROW'S WORKFORCE

The Nation's cyber infrastructure depends on well-trained Information Technology (IT) professionals to support the systems and networks necessary for essential computer operations. To increase this awareness of cybersecurity careers and academic pathways, the Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) Cyber Education Office (CEO) launched the Cyber Competitions Investigation Project (CCIP), which aims to develop a comprehensive list of all U.S. cyber competitions, which test the cybersecurity skills of participants. DHS believes that by encouraging hands-on learning in the cybersecurity field, the number of young people who will benefit - and who will consider entering the field of cybersecurity - will be multiplied.

PROJECT OVERVIEW

Cyber competitions are interactive, scenario-based events or exercises that help participating individuals develop cybersecurity skills and increase interest in cybersecurity careers. Cyber competitions foster talent in potential cybersecurity professionals that might otherwise be undetectable through traditional academic means, and encourage mentor-led atmospheres where participants can practice and hone cybersecurity skills in a controlled, real-world environment. DHS CEO aims to identify U.S.-based cyber competitions to analyze which cybersecurity knowledge, skills and abilities (KSAs) and specialty areas (SAs) the competitions test and promote, that are based on the National Cybersecurity Workforce Framework.

DHS CEO is a champion for all cyber competitions. CCIP aims to provide cyber competition administrators, participants, and sponsors with a wider view of other cyber competitions to increase involvement, and encourage recognition of the tremendous efforts of the teachers, competitors and coaches. DHS CEO will work with DHS Science and Technology (DHS S&T) to create a community repository outlining which KSAs and SAs of the Framework each cyber competition utilizes. DHS CEO's work will allow students the opportunity to pick a cyber competition that best fits their interests and needs to help them onto the Cybersecurity Highway, which defines various cybersecurity career pathways. Ultimately, the CCIP community repository will provide competitors, sponsors, administrators, and employers with a central source to find competitions in which to participate, fund, manage, or hire from.

CYBER COMPETITIONS GOALS & OBJECTIVES

In addition to the more specific objectives below, CCIP will socialize the Framework and ultimately strengthen the cybersecurity workforce. These specific objectives include:

1. Capturing and understanding the specific characteristics of existing cyber competitions on national, state and local scale based in high school, collegiate and post-collegiate academic levels.
2. Mapping current cyber competitions to the Framework.
3. Providing a central resource for cyber competition hosts.
4. Developing recommendations for DHS to further assist the collective efforts of these cyber competitions.

DHS CEO BACKGROUND

CEO leads the collaborative national effort to promote cybersecurity education, training, and workforce development to help the U.S. protect itself against future cybersecurity threats. CEO is located within DHS's National Protection and Programs Directorate (NPPD) National Cyber Security Division (NCSD) and plays a significant leadership role within the National Initiative for Cybersecurity Education (NICE). In this role, it works in partnership with other government agencies to support the development and maintenance of the Nation's cybersecurity workforce.



Education Opportunities

[Centers of Academic Excellence](#)
[Advanced Technological Education \(ATE\) Centers](#)
[Regional Cyber Centers](#)
[Integrated Cybersecurity Education Communities \(ICEC\)](#)

NICS Education Partners

[Stay Safe Online](#)
[Cyber Security Education Consortium \(CSEC\)](#)
[Center for Systems Security and Information Assurance \(CSSIA\)](#)
[DHS NCSD Software Assurance](#)

I Want To

[Become a Cyber Professional](#)
[Advance my Cyber Career](#)
[Explore the NICE Framework](#)
[Search for Training Courses](#)
[Get my child involved](#)
[Become a NICE Partner](#)
[Become a Training Catalog Vendor](#)

NICE Partners





TRAINING

Promoting Continuous Workforce Development

[Training Home](#)

[Training Catalog](#)

[Professional Certification](#)

[Sources](#)

[Call for Vendors](#)

[Mapping Instructions](#)

[Framework Download](#)

[NICE Initiatives](#)

[Workforce Development](#)

[Workforce Framework](#)



FIND COURSES

Search the most comprehensive listing of available Cybersecurity training.



GET CERTIFIED

A variety of professional certifications are available, find the one that fits your career goals.



DEVELOP TRAINING

Training strategies and guidance for businesses.



SUBMIT TRAINING

If you are a commercial or government agency you can register your Cyber & IA courses in the Training Catalog.

Why promote Cybersecurity training?

Securing, protecting, and defending our nation's digital information and associated systems and infrastructure require building and retaining an agile, highly skilled workforce that can respond flexibly to dynamic requirements. This is one of the foundational goals of the National Initiative for Cybersecurity Education (NICE). Building our nation's cybersecurity workforce requires two complimentary components: workforce planning and professional development. Workforce planning entails analyzing the capabilities needed to achieve the current mission and forecasting the capabilities that are needed in the future. Current and future talent gaps can be addressed through a combination of hiring, contracting, and professional development programs. [Learn more](#) about what NICE is doing to promote an agile workforce.

Explore the Workforce Framework

Experts across the country have begun the professionalization of the Cybersecurity domain. The first step in this effort was the development of a professional taxonomy, the [National Cybersecurity Workforce Framework](#), that identifies and categorizes areas of the Cybersecurity discipline. At this time each area has been mapped to the Federal Office of Personnel Management (OPM) Knowledge, Skills, and Abilities (KSA's). We are seeking the input of commercial industry to further develop the Framework. Find out how you and your organization can [participate and contribute](#).

Training Strategies for Businesses

No one knows your business like you do and developing tailored cybersecurity training will help keep your employees, environment, and clients secure, is a challenge. Explore [strategies for workforce development](#) that can help you identify skills gaps, identify appropriate training and create a thriving Cybersecurity Program.

TRAINING RESOURCES FOR FEDERAL EMPLOYEES

The following links are verified federal training sites and require authentication to access.

[Federal Virtual Training Environment \(FedVTE\)](#)

Federal employees can access a rich library of cybersecurity and information assurance training. Put yourself in the classroom to attend lectures, watch demonstrations, and conduct hands-on labs. View and manage your organization's website as they progress toward their training objectives.

[Federal Cybersecurity Training Events \(Fed CTE\)](#)

Federal employees can access hands-on training by "Red Team/Blue Team".

PUBLIC TRAINING VENDORS

The following vendors have registered their interest in the Training Catalog, but are not included by DHS.

[Training Company](#)

Computer security training, certification and other resources. We specialize in computer/network security, digital forensics, application security and IT audit.

[Cyber University](#)

Earn a cybersecurity degree online or onsite.

[Acme Business](#)

Providing technology and services to support homeland security, defense, and global health.

[Interested in participating? SUBMIT YOUR ORGANIZATION](#)



I Want To...

[Become a Cyber Professional](#)

[Advance my Cyber Career](#)

[Explore the NICE Framework](#)

[Search for Training Courses](#)

[Get my child involved](#)

[Become a NICE Partner](#)

[Become a Training Catalog Vendor](#)

NICE Partners



NIST



NICS

National Institute for Cybersecurity Studies

About NICS | A-Z Site Map



HOME

AWARENESS

EDUCATION

TRAINING

CAREERS

NEWS & EVENTS

RESEARCH

COMMUNITY

Training > Training Catalog > Search

THE TRAINING CATALOG

Catalog Search

Explore the Framework

Search 3,000+ Courses

By Specialty Area

Select one or more Specialty areas—
All Source Intelligence
Collection Operations
Computer Network Defense
Computer Network Defense Infrastructure Supp
Customer Service and Technical Support
Cyber Operations

By keyword

Enter a keyword

By Location

Enter a city or a zip

Limit distance by

5 mi

Search

Reset



Browse Courses
Using the Workforce Framework



I Want To..

Become a Cyber Professional

Advance my Cyber Career

Explore the NICE Framework

Search for Training Courses

Get my child involved

Become a NICE Partner

Become a Training Catalog Vendor

NICE Partners



NIST



Training > Training Catalog > Search

THE TRAINING CATALOG

Catalog Search

Explore the Framework

Filter Search

Refine Course Criteria

Keyword filter

Specialty Areas

Select specialty areas--

Customer Service and Technical Support

Provider

Select Provider--

Acme Training

Cyber University

Training Company

Reset

Filter

Records: 12 | Showing 1-10 | 11-20 | +1

Compare

Save Search

Telecommunications in Information Systems

view sessions

Training Company

WBT

An analysis of technical and managerial perspectives on basic concepts and applications in telecommunication systems. An overview of data communication protocols and standards, local area networks, etc.

Foundations of Information System Security

view sessions

Acme Training

WBT

A survey of various aspects of establishing and maintaining a practical cyber and information security program designed to protect key assets. Topics include physical and logical security mechanisms;

Networking Essentials

view sessions

Cyber University

CBT, WBT

An introduction to networking technologies for individual workstations, local area networks, wide area networks, and the Internet, with emphasis on the OSI (open system connectivity) model, security.

Network Security

view sessions

Cyber University

WBT

A study of the fundamental concepts of computer network security and their implementation. Topics include authentication, remote access, Web security, intrusion detection, basic cryptography, physical.

Information System Security Mechanisms

view sessions

Training Company

CBT

A hands-on technical examination of areas of security—such as authentication, authorization and access control, confidentiality, availability, data integrity (encryption), and nonrepudiation—that are.

Disaster Recovery Planning

view sessions

Cyber University

CBT

study of disaster recovery and emergency planning as applied to the information systems function in corporations. Topics include security risk evaluation and management, creation of threat profiles, ...

Information Security Needs Assessment and Planning

view sessions

Acme Training

CBT

In-depth practice in gathering security requirements to generate a security plan.

Network and Internet Security

view sessions

Cyber University

WBT

An introduction to the security concepts needed for the design, use and implementation of secure voice and data communications networks, including the Internet. A brief review of networking technology.

Computer Forensics

view sessions

Cyber University

WBT

An introduction to the fundamental concepts behind the collection and analysis of the digital evidence left behind in a digital crime scene.

EXPLORE THE FRAMEWORK

Customer Service and Technical Support



I Want To...

Become a Cyber Professional

Advance my Cyber Career

Explore the NICE Framework

Search for Training Courses

Get my child involved

Become a NICE Partner

Become a Training Catalog Vendor

NICE Partners





THE TRAINING CATALOG

Catalog Search

Explore the Framework

[Return to Search](#)

Telecommunications in Information Systems

[Learning Objectives](#) | [Available Sessions](#) | [Framework](#)

Description

An analysis of technical and managerial perspectives on basic concepts and applications in telecommunication systems. An overview of data communication protocols and standards, local area networks, wide area networks, and internetworks; and trends in telecommunications is provided. The implications of the regulatory environment and communications standards on transmission of voice, data, and image are examined.

Course Prerequisites : CSIA 301 Information System Architecture

Training Purpose : Continuing Education, Skill Development, Functional

Overall Course Level : Intermediate

Specific Audience:

Training Origin : Academic Institution

Learning Objectives

- Obtain an understanding of the overview of data communication protocols and standards; local area networks, wide area networks, and internetworks; trends in telecommunications; and the implications of the regulatory environment and communications standards on transmission of voice, data, and image.

This Course Fulfills the following KSAs

- Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools
- Knowledge of network architecture concepts including topology, protocols, and components
- Knowledge of network communication protocols such as TCP/IP, Dynamic Host Configuration, Domain Name Server (DNS), and directory services
- Knowledge of network security architecture, including the application of Defense-in-Depth principles
- Knowledge of network traffic analysis methods
- Knowledge of Open System Interconnection model
- Knowledge of packet-level analysis
- Skill in protecting a network against malware
- Skill in securing network communications
- Skill in using VPN devices and encryption

Categories:

- Analyze
- Investigate
- Operate and
- Collect
- Operate and
- Maintain
- Protect and
- Defend
- Securely
- Provision
- Support

Competencies:

- Computer Forensics
- Encryption
- Information Assurance
- Information
- Systems/Network
- Security
- Infrastructure Design
- Vulnerabilities
- Assessment

Provider

<http://www.acme.org>

Contact

1-800-123-4567

info@acme.org



I Want To...

[Become a Cyber Professional](#)

[Advance my Cyber Career](#)

[Explore the NICE Framework](#)

[Search for Training Courses](#)

[Get my child involved](#)

[Become a NICE Partner](#)

[Become a Training Catalog Vendor](#)

NICE Partners



NIST



[Training](#) > [Training Catalog](#) > [Search](#)

THE TRAINING CATALOG

[Catalog Search](#)

[Explore the Framework](#)

[Overview](#)

[Categories](#)

[Specialty Areas](#)

[KSAs](#)

[Competencies](#)

[Tasks](#)

About the Framework

The National Cybersecurity Workforce Framework classifies the typical duties and skill requirements of cybersecurity workers. The Framework is meant to define professional requirements in cybersecurity, much as other professions, such as medicine and law, have done. [\[Learn more about the Framework effort\]](#)

The Framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas. Within each category you'll find a list of specialty areas, clicking on a Specialty area will reveal the details about that area. Each specialty area detail displays the standard tasks and the Knowledge, Skills and Abilities (KSAs) needed to successfully complete those tasks. Select from any of the 7 areas (above or using the graphic at right) to browse the Framework Categories or use the job-title search box (at right).

Training and the Framework

Training is a foundational component for every workforce plan. By mapping courses to specific KSAs and Specialty Areas, Cyber Professionals, and those entering the Cyber Profession, can quickly identify the courses they need to meet the skill requirements of their position, advance within their specialty area, or transfer their skills to another position. Training providers have mapped their Courses are mapped to these KSAs so educational and training opportunities related to your specialty area can be quickly identified.

If you're an academic institution or training vendor and you like to map and submit your courses [\[click here\]](#), identify appropriate training and create a thriving Cybersecurity Program.



Not Sure Where You Fit in the Framework?

Enter your job title, or words that describe your major activities and let the Framework find you!

[Go](#)

Or browse the Categories using the Framework Graphic:



I Want To..

- [Become a Cyber Professional](#)
- [Advance my Cyber Career](#)
- [Explore the NICE Framework](#)
- [Search for Training Courses](#)
- [Get my child involved](#)
- [Become a NICE Partner](#)
- [Become a Training Catalog Vendor](#)

NICE Partners





Training > Training Catalog > Search

THE TRAINING CATALOG

Catalog Search

Explore the Framework

Overview

Categories

Specialty Areas

KSAs

Competencies

Tasks



View Related Courses

Information Assurance Compliance

[Related Job Titles](#) | [Tasks](#) | [KSAs](#)

DESCRIPTION

Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements. Ensures compliance from internal and external perspectives.

RELATED JOB TITLES

Persons working in this Specialty Area may have job titles similar to:

- Accreditor
- Validator
- IA Manager
- IA Officer
- Designated Accrediting Authority
- Certifying Official
- Certification Agent
- IA Compliance Analyst/Manager
- Auditor
- Security Control Assessor
- Authorizing Official Designated Representative
- Risk/Vulnerability Analyst
- Portfolio Manager
- Compliance Manager

TASKS

Professional involved in this Specialty perform the following tasks:

- Develop methods to monitor and measure compliance
- Develop specifications to ensure compliance with security requirements at the system or network environment level
- Draft statements of preliminary or residual security risks for system operation
- Maintain information systems accreditations
- Manage and approve Accreditation Packages (e.g., Defense Information Assurance Certification and Accreditation Process, National Information Assurance Certification and Accreditation Process, etc.)
- Monitor and evaluate a system's compliance with Information Technology security requirements
- Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks
- Plan and conduct security accreditation reviews for initial installation of systems and networks
- Provide an accurate technical evaluation of the application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant IACs
- Recommend new or revised security measures based on the results of security reviews
- Review accreditation documents to confirm that the level of risk is within acceptable limits for each network
- Verify that network/system security posture is implemented as stated, document deviations, and determine required actions to correct those deviations
- Verify that the network/system accreditation documentation is current

KSAs

Experts in the Specialty Area have the following Knowledge, Skills, and Ability:

- Knowledge of identified vulnerabilities, alerts, and bulletins (IAVA, IAVB)
- Knowledge of IT security certification and accreditation requirements
- Knowledge of IT security principles and regulations
- Knowledge of methods for evaluating, implementing, and disseminating IT security tools and procedures
- Knowledge of network architecture concepts including topology, protocols, and components
- Knowledge of pertinent government laws and information technology regulations
- Knowledge of structured analysis principles and methods
- Knowledge of systems diagnostic tools and fault identification techniques
- Knowledge of the organization's enterprise IT goals and objectives

Area Competency

- Enterprise Architecture
- Information Assurance
- Information Systems
- Security Certification
- Information Systems/Network Security
- Information Technology
- Performance Assessment
- Infrastructure Design
- Legal, Government and Jurisprudence
- Logical Systems Design
- Systems Testing and Evaluation



I Want To...

Become a Cyber Professional
Advance my Cyber Career
Explore the NICE Framework
Search for Training Courses
Get my child involved
Become a NICE Partner
Become a Training Catalog Vendor

NICE Partners





CAREERS

Driving Professionalization & Strategies for Talent Management

[Careers Home](#)

[Talent Management](#)

[Cyber Careers](#)

[Career Development](#)
[Career Roadmaps](#)

[NICE Initiatives](#)
[Professionalization](#)



MANAGE TALENT

Find, Attract and Retain Cyber Professionals



EXPLORE CAREERS

Browse the Possibilities using the National Cybersecurity Workforce Framework



WORKFORCE DEVELOPMENT

Learn about skills gap analysis, training strategies, and other activities to keep your Cyber workforce on top.



CAREER PLANNING

Career Roadmaps can help you plan your next move.

HR SITES

[Talent Management Institution \(TMI\)](#)
[National Association of Workforce Development Professionals \(NAWDP\)](#)

NICE WHITEPAPERS

[A Historical Review of How Occupations Become Professions](#)
[Best Practices for Planning a Cybersecurity Workforce](#)
[Best Practices for Implementing Professionalization](#)

Why Foster Professionalization and Career Development?

Cybersecurity is a relatively new occupational field in terms of formal qualifications, regulatory governance, and oversight. Therefore, the government is exploring the professionalization of cybersecurity by opening a national public conversation around the merits of professionalizing certain specialty areas of the National Cybersecurity Workforce Framework.

The Important Role of Talent Management

Talent Management is an all-encompassing term for strategic human capital activities that include recruitment/hiring, onboarding, engagement, succession planning, performance management, workforce planning, retention, leadership development, etc. It's about who you need, and how you get them - planning and execution. [\[Link to Talent Management page\]](#)

Career Spotlight

Interviews with cyber professionals, hiring managers and researchers. Highlighting their careers, how they got there, their thoughts on the profession, giving an "insiders" perspective.



I Want To...

[Become a Cyber Professional](#)
[Advance my Cyber Career](#)
[Explore the NICE Framework](#)
[Search for Training Courses](#)
[Get my child involved](#)
[Become a NICE Partner](#)
[Become a Training Catalog Vendor](#)

NICE Partners





NICS

National Institute for Cybersecurity Studies

About NICS | A-Z Site Map



HOME

AWARENESS

EDUCATION

TRAINING

CAREERS

NEWS & EVENTS

RESEARCH

COMMUNITY

Education Home

For Students

- Degree Programs
- Scholarship Opportunities
- Hands-On Learning Activities
- Cyber Competitions
- Cyber Camps

For Educators

NICE Initiatives

- STEM Improvement Efforts
- Common Evidence Standards
- Promoting Education
- Curriculum Resources
- Virtual Labs

Programs

- Software Assurance
- Centers of Academic Excellence (CAE)
- Regional Cyber Centers
- 1-Corps
- Scholarship for Service (SFS)
- Integrated Cybersecurity Education Communities (ICEC)
- Cyber Competitions
- Investigation Project (CCIP)

Education > NICE Initiative > CCIP

SOFTWARE ASSURANCE

Software Assurance Education Overview

Complex software systems affect nearly every aspect of our lives, in areas such as defense, government, energy, communication, transportation, manufacturing, and finance. Protecting these systems against vulnerabilities and attacks is critical, so there is a growing demand for skilled professionals who can build security and correct functionality into software and systems under development. Yet there are few software assurance programs or tracks that focus on developing assured software and, consequently, not enough professionals to meet the growing demand. The SwA Curriculum Project began in response to the growing demand for software assurance combined with the lack of professionals and educational programs to fill the need. The MSwA Reference Curriculum was created to guide institutions toward software assurance programs, beginning at the community college level and continuing through the master's program. [Learn More](#)

Workforce Education & Training Working Group

The Software Assurance Curriculum Project provides materials for undergraduate and graduate courses in software assurance. The Master of Software Assurance Reference Curriculum and Undergraduate Course Outlines reports and other resources are available for download.

Development of a Master of Software Assurance Reference Curriculum

Modern society is deeply and irreversibly dependent on software systems of remarkable scope and complexity in areas that are essential for preserving our way of life. The security and correct functioning of these systems are vital. Recognizing these realities, the U. S. Department of Homeland Security (DHS) National Cyber Security Division (NCS-D) enlisted the resources of the Software Engineering Institute at Carnegie Mellon University to develop a curriculum for a Master of Software Assurance degree program and define transition strategies for implementation. In this article, we present an overview of the Master of Software Assurance curriculum project, including its history, student prerequisites and outcomes, a core body of knowledge, and a curriculum architecture from which to create such a degree program. We also provide suggestions for implementing a Master of Software Assurance program.

The Master of Software Assurance Reference Curriculum is now recognized by the IEEE Computer Society and the Association for Computing Machinery. The IEEE Computer Society (IEEE-CS) and Association for Computing Machinery (ACM) have recognized the Master of Software Assurance (MSwA) Reference Curriculum as appropriate for a master's program in software assurance. This formal recognition signifies to the educational community that the MSwA Reference Curriculum is suitable for creating graduate programs or tracks in software assurance. The IEEE-CS and ACM have developed several computing curricula and are community leaders in curricula development. This MSwA curriculum includes focused curriculum recommendations for software assurance—the first curriculum developed for this specific field.

For sources, process, products, adoption strategies, and early adoption experiences related to the development of the Master of Software Assurance [see this paper](#).

VISIT THE PROGRAM SITE



MISSION

The Software Assurance (SwA) Workforce Education and Training Working Group is composed of members from industry, government, and academia and facilitates both existing and prospective (e.g., students and educational institutions) members of the workforce to improve their production of adequately secure software.



Education Opportunities

- Centers of Academic Excellence
- Advanced Technological Education (ATE) Centers
- Regional Cyber Centers
- Integrated Cybersecurity Education Communities (ICEC)

NICS Education Partners

- Stay Safe Online
- Cyber Security Education Consortium (CSEC)
- Center for Systems Security and Information Assurance (CSSSIA)
- DHS NCS-D Software Assurance

I Want To...

- Become a Cyber Professional
- Advance my Cyber Career
- Explore the NICE Framework
- Search for Training Courses
- Get my child involved
- Become a NICE Partner
- Become a Training Catalog Vendor

NICE Partners

